WHAT IS CLAIMED IS:

1. A method comprising:

receiving, by a verification system, from a computer in a blockchain network, a first data package for an event and a first digital signature associated with the first data package, the first data package including an event identifier and event information;

verifying, by the verification system, the first digital signature using a public key;

generating, by the verification system, a first block for a blockchain stored by the verification system, the first block including the first data package and the first digital signature;

verifying, by the verification system, that the event can be completed based on the event information;

in response to verifying that the event can be completed, generating, by the verification system, a second data package for the event, the second data package including the event identifier and information indicating that the event has been verified;

generating, by the verification system, a second digital signature for the second data package using a private key associated with the verification system;

generating, by the verification system, a second block for the blockchain, the second block including the second data package and the second digital signature; and

transmitting, by the verification system, the second data package and the second digital signature to one or more computers in the blockchain network.

2. The method of claim 1, wherein a coordination system receives the second data package, wherein the coordination system determines that the event has been verified based on the second data package, and wherein the coordination system causes the event to take place in response to determining that the event has been verified.

3. The method of claim 2, wherein ~~a~~ the coordination system causes the event to take place by transmitting a message to the verification system, and the method further comprising:

receiving, by the verification system, from the coordination system, a message instructing the verification system to execute the event; and

executing the event.

4. The method of claim 2, further comprising:

receiving, by the verification system, from the coordination system, a third data package for the event and a third digital signature associated with the third data package, the third data package including the event identifier and information indicating the event has been completed;

verifying, by the verification system, the third digital signature using a second public key associated with the coordination system; and

generating, by the verification system, a third block for the blockchain stored by the verification system, the third block including the third data package and the third digital signature.

5. The method of claim 1, wherein the blockchain network includes a plurality of peer computers, and wherein each peer computer builds and stores a copy of the blockchain.

6. The method of claim 5, wherein the private key is a second private key, wherein the first data package is received from a first peer computer of the plurality of peer computers, wherein the first digital signature was generated with a first private key associated with the first peer computer, and wherein the public key is a first public key associated with the first peer computer.

7. The method of claim 6, wherein verifying that the event can be completed includes:

identifying an account associated with the first peer computer; and

determining that the event as described by the event information can be completed based on the account.

8. The method of claim 6, wherein the verification system includes a verification computer, an adaptor computer, and a second peer computer of the plurality of peer computers.

9. The method of claim 8, wherein the plurality of peer computers compose a first blockchain network channel, wherein the blockchain is a first blockchain associated with the first blockchain network channel, wherein the second peer computer also participates in a second blockchain network channel, wherein the first blockchain network channel and the second blockchain network channel do not have the same set of peer computers, and wherein a second blockchain is associated with the second blockchain network channel, the second blockchain being different than the first blockchain.

10. The method of claim 1, wherein the event information includes a sender identifier and a receiver identifier.

11. A verification system comprising:

at least one processor; and

at least one computer readable medium, the at least one computer readable medium comprising code, executable by the processor, for implementing a method comprising:

receiving, from a computer in a blockchain network, a first data package for an event and a first digital signature associated with the first data package, the first data package including an event identifier and event information;

verifying the first digital signature using a public key;

generating a first block for a blockchain stored by the verification system, the first block including the first data package and the first digital signature;

verifying that the event can be completed based on the event information;

in response to verifying that the event can be completed, generating a second data package for the event, the second data package including the event identifier and information indicating that the event has been verified;

generating a second digital signature for the second data package using a private key associated with the verification system;

generating a second block for the blockchain, the second block including the second data package and the second digital signature; and

transmitting the second data package and the second digital signature to one or more computers in the blockchain network.

12. The verification system of claim 11, wherein a coordination system receives the second data package, wherein the coordination system determines that the event has been verified based on the second data package, and wherein the coordination system causes the event to take place in response to determining that the event has been verified.

13. The verification system of claim 12, wherein ~~a~~ the coordination system causes the event to take place by transmitting a message to the verification system, and the method further comprising:

receiving, by the verification system, from the coordination system, a message instructing the verification system to execute the event; and

executing the event.

14. The verification system of claim 12, further comprising:

receiving, by the verification system, from the coordination system, a third data package for the event and a third digital signature associated with the third data package, the third data package including the event identifier and information indicating the event has been completed;

verifying the third digital signature using a second public key associated with the coordination system; and

generating a third block for the blockchain stored by the verification system, the third block including the third data package and the third digital signature.

15. The verification system of claim 11, wherein the blockchain network includes a plurality of peer computers, and wherein each peer computer builds and stores a copy of the blockchain.

16. The verification system of claim 15, wherein the private key is a second private key, wherein the first data package is received from a first peer computer of the plurality of peer computers, wherein the first digital signature was generated with a first private key associated with the first peer computer, and wherein the public key is a first public key associated with the first peer computer.

17. The verification system of claim 16, wherein verifying that the event can be completed includes:

identifying an account associated with the first peer computer; and

determining that the event as described by the event information can be completed based on the account.

18. The verification system of claim 16, wherein the at least one processor includes a first processor, a second processor, and a third processor, and wherein the at least one computer readable medium includes a first computer readable medium, a second computer readable medium, and a third computer readable medium, and wherein the verification system further includes:

a verification computer including the first processor and the first computer readable medium;

an adaptor computer that including the second processor and the second computer readable medium; and

a second peer computer of the plurality of peer computers, the second peer computer including the third processor and the third computer readable medium.

19. The verification system of claim 18, wherein the plurality of peer computers compose a first blockchain network channel, wherein the blockchain is a first blockchain associated with the first blockchain network channel, wherein the second peer computer also participates in a second blockchain network channel, wherein the first blockchain network channel and the second blockchain network channel do not have the same set of peer computers, and wherein a second blockchain is associated with the second blockchain network channel, the second blockchain being different than the first blockchain.

20. The verification system of claim 11, wherein the event information includes a sender identifier and a receiver identifier.

21. A method comprising:

receiving, by a coordination system, from a computer in a blockchain network, a second data package for an event and a second digital signature associated with the second data package, the second data package including an event identifier and information indicating that the event has been verified;

verifying, by the coordination system, the second digital signature using a public key;

generating, by the coordination system, a second block for a blockchain stored by the coordination system, the second block including the second data package and the second digital signature;

causing, by the coordination system, the event to be executed;

generating, by the coordination system, a third data package for the event, the third data package including the event identifier and information indicating that the event has been executed;

generating, by the coordination system, a third digital signature for the third data package using a private key associated with the coordination ~~verification~~ system;

generating, by the coordination system, a third block for the blockchain, the third block including the third data package and the third digital signature; and

transmitting, by the coordination system, the third data package and the third digital signature to one or more computers in the blockchain network.

22. A coordination system comprising:

at least one processor; and

at least one computer readable medium, the at least one computer readable medium comprising code, executable by the processor, for implementing a method comprising:

receiving, from a computer in a blockchain network, a second data package for an event and a second digital signature associated with the second data package, the second data package including an event identifier and information indicating that the event has been verified;

verifying the second digital signature using a public key;

generating a second block for a blockchain stored by the coordination system, the second block including the second data package and the second digital signature;

causing the event to be executed;

generating a third data package for the event, the third data package including the event identifier and information indicating that the event has been executed;

generating a third digital signature for the third data package using a private key associated with the coordination ~~verification~~ system;

generating a third block for the blockchain, the third block including the third data package and the third digital signature; and

transmitting the third data package and the third digital signature to one or more computers in the blockchain network.